Entrance and Exit Criteria for JITF Integration Testing

ENTRY CRITERIA

Department of Defense Intelligence Information System (DoDIIS) Certification testing including Joint Integration Test Facility (JITF) integration testing applies to all DoDIIS operating at more than one location.

The following items list the steps that must be completed or products that must be delivered before integration testing will begin at the JITF. These items are more thoroughly discussed in the *Test and Evaluation Policy for Department of Defense Intelligence Information System (DoDIIS) Intelligence Mission Applications (IMA).*

Failure to meet all entry criteria is grounds to postpone or cancel testing for an IMA. Prior to the scheduled start date for integration testing, the JITF will notify the IMA PMO if any entry criterion has not been met and if the scheduled start date for testing has been moved because of the missing criterion.

All information, forms, and checklists are available on the JITF web site at http://www.if.afrl.af.mil/programs/jitf/, and are also provided in hardcopy format during the Joint Test Planning Meeting (JTPM) by the JITF Representative assigned to the IMA PMO.

1. Joint Test Planning Meeting

The JTPM is the formal start point of the certification testing process. Milestones that must be met for testing are identified as a result of this meeting.

A JITF representative will be assigned to the IMA PMO at this meeting to coordinate all DoDIIS Beta I (JITF, Security Certification, and Joint Interoperability Test Command [JITC]) activities.

JTPMs can be scheduled by contacting the DoDIIS Executive Agent for Test and Evaluation (DExA for T&E) at 757-225-3608 or DSN 575-3608 at least three months prior to anticipated JITF test dates.

2. In-Plant Acceptance Testing

Functional certification (In-Plant Acceptance Testing – IPAT) is the responsibility of the PMO. The JITF will verify that this certification is accomplished prior to the start of JITF testing. The IMA enters JITF testing upon successful completion of IPAT.

a) The PMO shall certify in writing to the DExA for T&E (electronic mail is acceptable: dexa.te@langley.af.mil) that the IMA has successfully completed IPAT by the Joint Test Readiness Review (normally five to ten days prior to test start). The IPAT certification letter shall include:

- A statement that DoDIIS IMA functionality satisfied the Requirements Definition Documentation and that all required functional capabilities are implemented and tested;
- A statement that DoDIIS IMA functionality satisfied the Requirements Traceability Matrix;

- A listing of interfaces tested;
- An attachment containing the IPAT Test Plan, Procedures, and Report with the outstanding related deficiencies (with deficiency code assigned) and schedule of planned fixes;
- Verification that the software was successfully installed and identification of the documentation used to complete the installation and personnel conducting the installation

b) The PMO shall certify that all IPAT Code 1 and 2 findings are closed and that all IPAT Code 3 findings are scheduled for disposition. An IPAT letter template is provided in the Information Package provided at the JTPM and is available on the JITF web site.

3. JITF Work Plan

The JITF Work Plan is provided to the IMA PMO at the JTPM. The PMO shall complete the Work Plan and return it to the JITF Representative no later than 45 days prior to the tentatively scheduled test start date. Work Plan templates are also available on the JITF web site.

4. Delivery of Software Baseline

The IMA baseline shall be delivered to the JITF Representative by the JTRR. The software baseline submitted by the PMO to the JITF shall be frozen until all tests are complete. No changes will be made to the baseline during JITF testing.

5. Delivery of Documentation

IMA documentation and information shall be delivered to the JITF Representative no later than 14 days prior to the anticipated test dates. The PMO shall provide the types of documentation identified below. Specific formats are not required for documentation with the exception of Security related information.

Document Type	**Information Content**
Requirements Definition Documentation	Provides written requirements for the IMA
Requirements Traceability Matrix	Traces requirements through program documentation
Security Accreditation Documentation	Provides information in accordance with the DODIIS Developer's Guide for Automated Information Systems (AIS) Security in Intelligence Information Systems, November 1993
Test Plans, Procedures and Test Reports	Provides information as described in IEEE /EIA Standard 12207
Interface Control Document	Provides detailed information on interfaces between applications
Software Version Description	Provides information regarding the software version, including changes and known problems

User Documentation	Users manuals, operator guides
Configuration and Installation Guide	Provides software installation instructions
Transition Plans	Transition details for software upgrades, data base changes, future direction for requirements and design of software application
Open Problem Reports	Required no later than the Joint Readiness Review (JTRR)

Documents that do not appear on the above list but which are deemed necessary for testing shall be identified at the JTPM and delivered to the JITF no later than 14 days prior to the start of testing.

6. Receipt of Clearances

Clearances for IMA PMO support personnel participating in the JITF test must be provided in advance. Information on where to pass clearances will be provided by the JITF representative assigned to the program undergoing testing.

EXIT CRITERIA

A positive evaluation of an IMA during JITF testing is based in large part on the extent that the IMA meets the requirements documented in the *DODIIS INTEGRATION REQUIREMENTS and EVALUATION Version 4.2*, published by the JITF.

To receive a recommendation from the JITF to proceed to the next step in the DODIIS Certification Process (Beta II testing at an operational site) the following criteria must be met:

1. Satisfy 75% of applicable integration requirements
2. Have no open Impact Code 1 findings
3. Have no open Security Category I or II findings for requirement INT-SEC 20, which states:

   Upon successful completion and verification of the application installation, a security risk analysis will be conducted to target system vulnerabilities

4. All security documentation developed in support of the application is available on Security Virtual Test Folder (SVTF) located on Intelink at (http://web1.rome.ic.gov/svtf). The availability of this documentation on the SVTF, in final form, also factors into the DODIIS Executive Council's (DEC) fielding decision for the application.

The integration requirements identify technical areas of software installation, configuration, and use that influence the IMA's effects on other applications and on the site operating environment. The integration requirements are organized by category:

Entrance and Exit Criteria for JITF Integration Testing

- Documentation - These requirements evaluate the content and structure of IMA documents that the system administrator/installer will rely on to plan the IMA's resource requirements and to determine the effects of the software on the operational and security architectures of the site.
- Installation and Configuration - These requirements evaluate the IMA's installation process and the steps required to configure the IMA for use.
- Environment - These requirements evaluate the operating environment established or required by the IMA when it begins execution and the potential effects of that environment on other applications.
- Operation - These criteria examine aspects of the execution of the IMA that could affect the execution, configuration, or security of other applications, either on the same hardware platform or on other platforms at the site. Included in this category is how administration of the IMA integrates into the overall system administration strategy of a site.
- User Interface - These criteria are concerned with the integration of the IMA with the windowing system of the workstation.
- Security - These objectives identify areas of the design and operation of the IMA that may affect the site security architecture. These objectives may address areas of system security architecture that are not identified in the IMA security documentation.

The JITF evaluates the extent to which the IMA meets each requirement. For each requirement that the IMA does not meet, the JITF documents one or more findings and assesses an impact level for each finding.

Not all of the integration requirements have equal weight. That is, the failure to meet some requirements has more significance than the failure to meet other requirements. In addition, the design of the IMA will also influence the significance of unmet requirements. The appropriate range of impact codes is provided for each requirement in the *Joint Integration Test Facility (JITF) DoDIIS Integration Requirements and Evaluation Procedures Version 4.2*.

A successful evaluation means that the IMA has passed integration certification, and the JITF will recommend that the IMA proceed to the next step in the IMA certification process. An unsuccessful evaluation means that the IMA has failed integration certification, and the JITF will recommend that the IMA not proceed to the next step in the IMA certification process.

Entrance and Exit Criteria for JITF Integration Testing

DODIIS INTEGRATION IMPACT CODES

The following codes are used by the JITF to indicate the impact or significance of each integration finding.

Impact Code 1

A finding that,

a) identifies baseline adjustments, not included in the installation guide, made during the test event in order to successfully install the application;

b) has a serious effect on the operation of either the application or on another application or component of the infrastructure; or

c) impacts cost, schedule, performance or Post-Deployment Software Support (PDSS).

d) identifies a security vulnerability in the application or site architecture that can be exploited by a general user; or

e) seriously increases the level of effort required by site personnel to manage the application or other applications.

An Impact Code 1 finding is assigned if the application baseline must be changed in order to continue testing, if the installation documentation is not detailed enough to support the successful installation of the application, or if a security vulnerability exists.

The level of effort is a key determinant for Impact Code 1 findings. The time or expertise that is required to install or manage the application cannot exceed what is reasonably expected for an application. For example, if the installation guide says that the application can be installed in a single day, but the installation takes more than 20 working hours, then an Impact Code 1 finding would be generated.

An application cannot proceed to Beta II testing until all Impact Code 1 findings have been resolved by the PMO and verified by the JITF Engineers.

Impact Code 2

A finding that,

a) has a significant effect upon, but does not prevent, the successful installation of the application under evaluation;

b) has a significant effect on the operation of either the application or on another application or component of the infrastructure;

c) impacts cost, schedule, performance or Post-Deployment Software Support (PDSS).

d) creates a security vulnerability in the application; or

e) significantly increases the level of effort required by site personnel to manage the application or other applications.

An Impact Code 2 finding can be resolved by a change in procedure or configuration. The resolution of an Impact Code 2 finding requires a significant level of effort by site administrators. The resolution does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF or NIMA ITF.

Impact Code 2 findings do not cause integration test failure, but the accumulation of Impact Code 2 findings may affect the test organization’s “go/no go” recommendation.

Impact Code 3

A finding that,

a) has an effect upon the installation of the application under evaluation;

b) has a effect on the operation of either the application or on another application or component of the infrastructure; or

c) increases the level of effort required by site personnel to manage the application or other applications, but does not require a significant level of effort by site administrators.

The successful resolution of an Impact Code 3 finding requires technical expertise expected of site administrators. The resolution does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF or NIMA ITF.

Impact Code 3 findings do not cause integration test failure, but the accumulation of Impact Code 3 findings may affect the test organization’s “go/no go” recommendation.

Impact Code 4

A finding that,

a) has little or no effect upon the installation of the application under evaluation;

b) has a little effect on the operation of either the application or on another application or component of the infrastructure; or

c) nominally increases the level of effort required by site personnel to manage the application or other applications, but does not require a significant level of effort by site administrators.

The finding can be resolved by a workaround that can be implemented as a change in during integration testing without a significant level of effort, or the finding can be left as is. Even though the finding has some effect on the configuration or operation of the mission application, or on other components of the site architecture the administrator will be able to manage the mission application.

DIA/SYE-3C SECURITY CATEGORY CODES

Category I

A significant deficiency that must be corrected before the system can become operational or must be fixed before an operational system can continue to operate. Examples include findings that give administrator/root privileges to manipulate the system (i.e., change the configuration, remotely execute commands as root, etc.) to unauthorized and/or unauthenticated users. (JITF tools will identify Category I and II security findings as Impact Code 1 SFs)

Category II

A security related deficiency that must be corrected within a specified period in order to continue system operation. Examples include many configuration mistakes, most excessive services, vulnerabilities that may deny service without any other side effects, system information provided to unauthenticated users, many violations of need-to-know and least privileges. (JITF tools will identify Category I and II security findings as Impact Code 1 SFs)

Category III

A security relevant recommendation for which the implementation is a command or program office option. Examples include areas where another, more secure method of implementing a function of the system, such as updates that add new security features or enabling a security feature. (JITF tools will identify Category III security findings as Impact Code 3 SFs)

Category IV

A non-security relevant recommendation for which the implementation is a user command or program office option. Examples include patches or updates that may improve performance or ease administration. The JITF will not identify any Category IV findings as part of this annex. Findings of this nature will be reported in the JITF Test Report for the application under evaluation using the appropriate JITF Impact Code levels.